DINAMIKA REKAYASA
http://dinarek.unsoed.ac.id
Vol. 14 No. 1 (2018) Hal. 57-64
p-ISSN 1858-3075 | e-ISSN 2527-6131

TEKNIK SUPER ENKRIPSI MENGGUNAKAN TRANSPOSISI KOLOM BERBASIS *VIGENERE CIPHER* PADA CITRA DIGITAL

SUPER ENCRYPTION TECHNIQUE USING TRANSPOSITION COLUMN BASED ON VIGENERE CIPHER ON DIGITAL IMAGE

Daurat Sinaga*, Chaerul Umam, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto

*Email: dauratsinaga@dsn.dinus.ac.id

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro, Semarang

Abstrak— Meretas data atau sering disebut *hacking* saat ini marak terjadi dalam internet, sehingga menyebabkan proses pengiriman data menjadi tidak aman. Oleh karena itu, diperlukan suatu sistem keamanan untuk mengamankan data ketika akan berkirim pesan antar satu dengan lainnya. Kriptografi merupakan salah satu sistem keamanan dengan konsep membuat data tersebut menjadi sandi - sandi yang tidak setiap orang dapat membacanya. Di dalam kriptografi terdapat berbagai macam algoritma untuk menyandikan sebuah data tersebut agak tidak mudah terbaca oleh orang lain yang tidak berhak, yaitu antara lain *vigenere cipher* dan transposisi kolom. Dengan mengkombinasikan algoritma inididapatkan teknik super enkripsi yang kuat yang dapat mengamankan data yang akan dikirimkan oleh pengirim kepada penerima tanpa diketahui oleh orang lain. Hasil eksperimen menunjukkan bahwa waktu enkripsi tercepat diperoleh gambar Lena dengan ukuran 128x128 piksel pada 0,100510 detik sedangkan waktu tertinggi untuk enkripsi yaitu untuk ukuran 1024x1024 piksel yang memerlukan waktu 10,148356 detik. Pada hasil dekripsi pesan, nilai PSNR tertinggi yaitu *inf* yang berarti citra tersebut telah memenuhi aspek keamanan dimana nilai *inf* diartikan bahwa citra asli dan citra hasil dekripsi tidak mengalami perubahan sama sekali. Di sisi lain, dari hasil dekripsi dibutuhkan waktu yang relatif lebih lama dibanding proses enkripsi.

Kata kunci— Kriptografi, *vigenere*, transposisi kolom, enkripsi, keamanan pesan.

Abstract— Hacking data or often called hacking is currently happening in the internet, thus causing the process of sending data to be unsafe. Therefore, we need a security system to secure our data when it will send messages to each other. Cryptography is one of the security systems with the concept of making the data into passwords - a password that not everyone can read it. In cryptography there are various algorithms to encode a data is somewhat not readable by others who are not entitled, namely among others vigenere cipher and transposition column. By combining this algorithm we get a powerful super-encryption technique that can secure data that will be sent by the sender to the recipient unnoticed by others.The experimental results show that the fastest encryption time is obtained by Lena image with size 128x128 pixels at 0.100510 sec while the highest time for encryption is for 1024x1024 pixels which takes 10.148356 sec. On the decryption of the message, the highest PSNR value is inf which means the image has full filled the security aspect where the inf value means that the original image and the decrypted image have not changed at all. On the other hand, from the decryption takes a relatively longer time than the encryption process.

Keywords— Cryptography, Vigenere, column transposition, encryption, message security.

I. PENDAHULUAN

Kegiatan meretas data atau sering disebut *hacking* saat ini marak terjadi dalam internet, di sisi lain masyarakat sebagai pemilik data tidak mengatahui bahwa data yang mereka miliki telah diambil oleh orang lain [1]. Pada suatu waktu data tersebut dapat menjadi data rahasia yang tidak boleh diketahui oleh orang lain. Sebagian kecil dari masyarakat yang merupakan peneliti kini telah mengembangkan teknik yang dapat digunakan untuk mengamankan data-data tersebut. Teknik itu salah satunya bernama kriptografi.

Teknik kriptografi telah dilakukan dalam media teks pada beratus tahun yang lalu. Seiring berkembangnya teknologi, kriptografi membutuhkan algoritma yang kuat. Kriptografi dilakukan dengan tujuan proteksi data [2]. Sebagai hasil dari proses kriptografi, data akan terlihat rusak dan tidak dapat dibaca [3]. Pada teknik kriptografi klasik, ada dua macam teknik dasar yaitu substitusi dan transposisi. Teknik substitusi dapat dilakukan dengan operasi *monoalphabetic* dan *polyalphabetic* yang biasanya menggunakan media teks atau dokumen. Pada kriptografi teks, dapat digunakan algoritma substitusi *cipher* misalnya *Blowfish, Twofish, Vernam Cipher, Vigenere Cipher, Beaufort Cipher* atau *Autokey Cipher*. Penelitian yang telah dilakukan oleh Fahrianto [4] menggunakan algoritma *Vigenere Cipher* pada media teks dapat dilakukan dengan mudah. Namun terdapat kekurangan dalam pengimplementasian *Vigenere Cipher*.

Vigenere cipher merupakan algoritma yang cepat dan dapat dilakukan dengan menggunakan tabel alfabet yang disebut *tabula recta*, *Vigenere square*, atau tabel *vigenere*. Tabel tersebut terdiri dari alfabet yang ditulis 26 kali dalam baris yang berbeda, masing-masing alfabet bergeser ke kiri dibandingkan dengan alfabet sebelumnya, sesuai dengan 26 kemungkinan *ciphers caesar*. Pada titik yang berbeda dalam proses enkripsi, cipher menggunakan alfabet yang berbeda dari salah satu baris [5]. Alfabet yang digunakan pada setiap titik bergantung pada kata kunci yang berulang [6]. Namun kunci yang digunakan masih dapat dipecahkan baik secara *brute force* maupun menggunakan *software* tertentu. Algoritma *vigenere* merupakan salah satu algoritma kriptografi sandi abjad majemuk. Untuk meningkatkan keamanan, maka dalam penelitian ini teknik substitusi pada *vigenere cipher* akan dikombinasikan dengan teknik transposisi kolom. Transposisi kolom dipilih karena dapat digunakan untuk mengacak kembali posisi *cipherteks* [5] hasil *vigenere cipher*. Penggunaan transposisi kolom dengan kunci yang berbeda dengan kunci yang digunakan pada proses penyandian Vigenere cipher akan meningkatkan keamanan [7]. Penelitian yang dilakukan oleh Kester [8], telah melakukan peningkatan performa *vigenere cipher* dengan melakukan variasi pada kunci yang digunakan. Hal ini bertujuan agar *ciphertext* dapat memiliki pola kunci enkripsi yang berbeda dan kriptosistem Vigenère akan lebih sulit untuk diuraikan menggunakan serangan frekuensi. Penelitian lain yang dilakukan oleh Soofi dkk [9], melakukan peningkatan proteksi data pada *vigenere cipher* menggunakan modulo 27, dimana terdapat gabungan antara karakter *plainteks* dan karakter frase kunci.

Saat ini kriptografi tidak hanya dilakukan pada file teks saja, tapi dimungkinkan juga pada citra digital. Ada beberapa metode kriptografi yang dikhususkan hanya untuk mengenkripsi citra saja, tapi ada pula metode yang dapat bekerja pada teks maupun citra. Metode *vigenere cipher* dan transposisi kolom juga memungkinkan untuk dapat bekerja pada citra digital Dengan menggabungkan *vigenere cipher* dan tranposisi kolom maka akan didapat teknik super enkripsi yang lebih aman. Maka pada penelitian ini teknik super enkripsi diterapkan pada citra digital.

II. TINJAUAN PUSTAKA

A. Kriptografi

Menurut Katz [10], kriptografi dikaitkan dengan proses mengubah teks biasa menjadi teks yang tidak dapat dipahami dan sebaliknya. Ini adalah metode untuk menyimpan dan mentransmisikan data dalam bentuk tertentu sehingga hanya untuk siapa yang dimaksudkan dapat membaca dan memprosesnya [10]. Kriptografi tidak hanya melindungi data dari pencurian atau perubahan, namun juga dapat digunakan untuk otentikasi pengguna.

Tujuan dari kriptografi adalah untuk melindungi data yang ditransmisikan dalam kemungkinan adanya penyalahgunaan data, sehingga kriptografi adalah prosedur dimana data teks biasa disamarkan, atau dienkripsi, menghasilkan teks yang diubah, yang disebut *ciphertext*, yang tidak mengungkapkan yang asli memasukkan [11]. *Ciphertext* dapat diubah secara terbalik oleh penerima yang ditunjuk sehingga *plaintext* asli dapat dipulihkan. Kriptografi memainkan peran penting dalam hal *authentication*, kerahasiaan data, integritas data dan *non repudiation* [12].

B. *Vigenere Cipher*

Vigenere cipher adalah metode untuk mengenkripsi teks alfabet dengan menggunakan serangkaian caesar cipher yang berbeda berdasarkan huruf-huruf kata kunci. Ini adalah bentuk sederhana dari substitusi *polyalphabetic* [4]. *Vigenere cipher* merupakan salah satu bentuk kriptografi yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, atau sering disebut dengan kunci simetris. Dalam penyandiannya, *vigenere* menggunakan fungsi modulo. Kunci yang random dan memiliki panjang yang sama dengan *plaintext*

akan membuat metode ini sulit dipecahkan [1]. Pada penelitian ini format ASCCI akan digunakan untuk mengkonversi teks dimana rentang nilai desimal hasil konversi ASCCI yang digunakan hanya 0-255 maka digunakan persamaan (1) untuk proses enkripsi dan persamaan (2) untuk proses dekripsi berikut ini.

$$C(z) = \big(P(z) + K(z)\big) mod\ 256 \quad (1)$$
$$P(z) = \big(C(z) + K(z)\big) mod\ 256 \quad (2)$$

Dimana:
C = teks *cipher*
P = *plaintext*
K = kunci
z = indeks

C. Teknik Transposisi Kolom

Tidak seperti *cipher* substitusi sederhana (seperti *caesar cipher*), yang mengubah huruf pesan di sekitar, *cipher* transposisi *r* malah bekerja dengan mengotak-atik urutan huruf untuk menyembunyikan pesan yang sedang dikirim [13]. Model operasi algoritma ini mirip dengan anagram, namun dengan struktur yang lebih teratur sehingga bisa didekripsi dengan mudah.

Plaintext : INI ADALAH PESAN RAHASIA!
Kata Kunci : ZEBRAS → 6 3 2 4 1 5

6	3	2	4	1	5
I	N	I		A	D
A	L	A	H		P
E	S	A	N		R
A	H	S	I	A	!

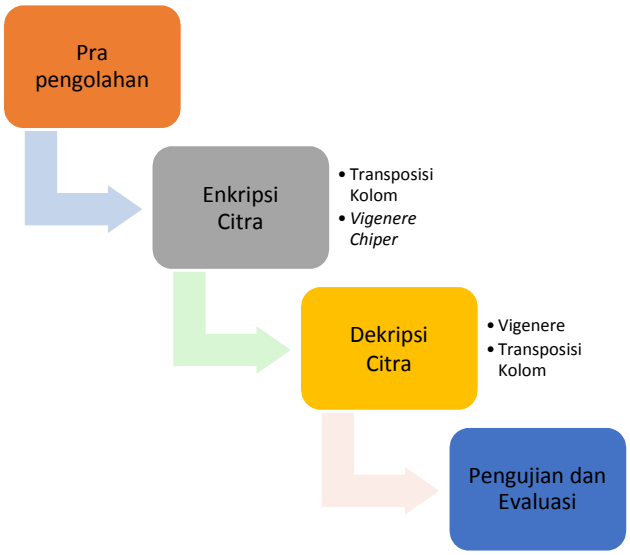
Cipher Teks : A AIAASNLSH HNIDPR!IAEA

Gambar-1. Proses enkripsi dengan metode transposisi kolom.

Dalam transposisi kolumnar, pesan ditulis dalam barisan dengan panjang yang tetap, dan kemudian membacanya lagi kolom demi kolom, dan kolomnya dipilih dalam beberapa ordo orak-arik[14]. Baik lebar baris dan permutasi kolom biasanya ditentukan oleh kata kunci. Misalnya, kata ZEBRAS berukuran panjang 6 (jadi barisnya adalah panjang 6), dan permutasi didefinisikan menurut urutan alfabet huruf dalam kata kunci. Dalam hal ini, pesanannya adalah "6 3 2 4 1 5". Dalam transposisi ini, teks biasa hanya ditempatkan dalam format kolom seperti apa adanya. Tapi, dalam tulisan ini ada penggunaan konsep ROT-13 ke teks biasa sebelum dikonversi menjadi bentuk matriks. Bahkan Algoritma ini juga bisa mengubah nilai numerik sekaligus karakter spesial. Gambar 1 adalah ilustrasi dari algoritma transposisi kolom.

III. METODE

Berikut adalah metode yang digunakan dalam implementasi kombinasi metode transposisi kolom dan *vigenere cipher* untuk mengamankan file teks, untuk lebih jelasnya dapat melihat Gambar-2.

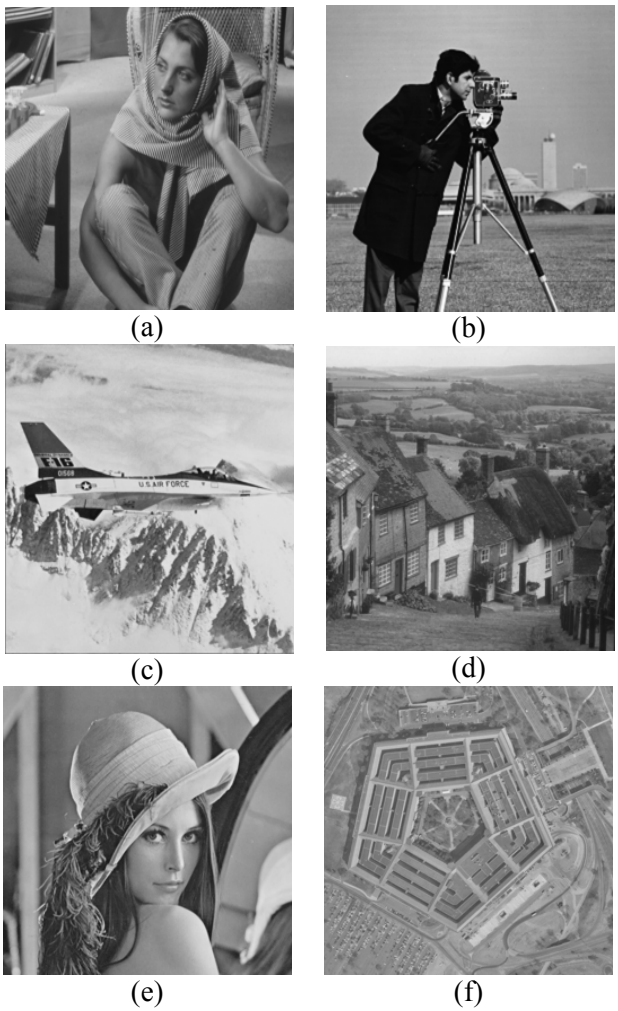


Gambar-2. Tahapan dalam metode yang digunakan.

A. Pra-Pengolahan

Setelah melakukan analisa maka dalam penelitian ini digunakan kombinasi metode transposisi kolom dan *vigenere cipher* untuk membuat teknik super enkripsi. Teknik ini akan dilakukan pada citra digital. Citra akan diolah menggunakan *software* matlab. Citra yang digunakan adalah citra keabuan dimana ukuran citra yang digunakan bervariasi dari 128*128, 256*256, 512*512, 1024*1024 dengan panjang kunci berupa teks huruf berkisar 6 karakter hingga 100 karakter.

Citra gambar yang diujicobakan pada studi ini menggunakan citra gambar yang sudah biasa digunakan dalam analisa pengolahan citra dari http://www.petitcolas.net/watermarking/image_data base.



(a) (b) (c) (d) (e) (f)

Gambar-3. Citra digital yang akan diujicobakan {(a) *Barbara*; (b) *Cameraman*; (c) F16; (d) Goldhill; (e) Lena; (f) Pentagon}.

B. Enkripsi Citra

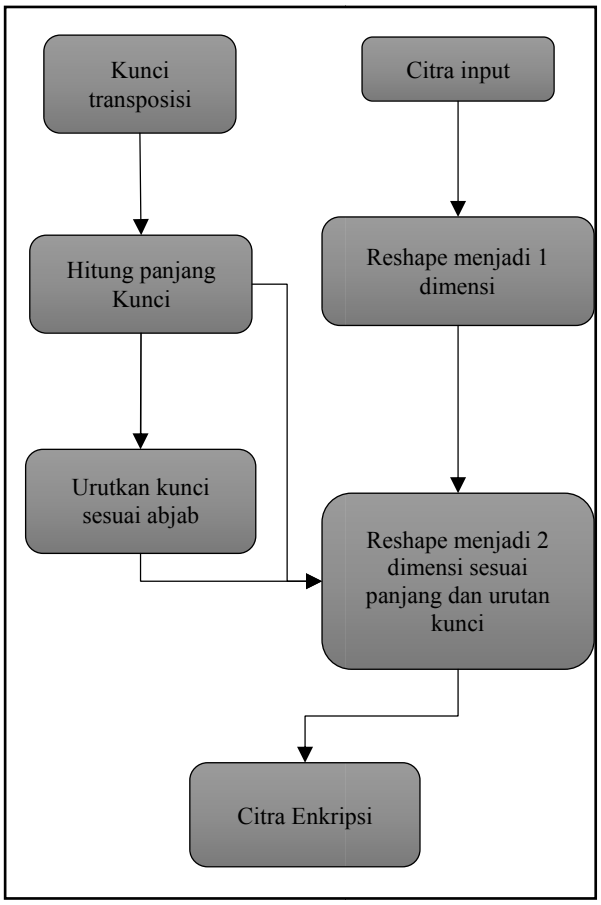
Pada tahap enkripsi citra dilakukan dengan mengkombinasikan dua metode yaitu transposisi kolom dan dilanjutkan dengan *vigenere cipher*. Proses ini dilakukan oleh pengirim pesan.

1) Enkripsi tranposisi kolom pada citra

Algoritma enkripsi transposisi kolom, saat ini memang banyak digunakan pada file teks, tapi pada penelitian ini akan diterapkan citra digital. Hasil enkripsi dengan transposisi kolom akan mengubah citra menjadi satu dimensi. Gambar 4 menunjukkan alur proses enkripsi tranposisi kolom pada citra.

Berikut adalah langkah detil dari proses enkripsi citra dengan transposisi kolom.

1. Baca citra input yang akan dienkripsi.
2. Ubah citra menjadi satu dimensi atau *array*.
3. Inputkan kunci berupa teks yang terdiri dari huruf dengan panjang berkisar 6-10 karakter
4. Ubah kembali citra satu dimensi menjadi satu dimensi dengan jumlah kolom pajang karakter dan baris menyesuaikan.
5. Urutkan kunci sesuai abjab, lalu ubah citra menjadi satu dimensi sesuai dengan urutan abjad kunci.
6. Dapatkan citra terenkripsi.



Gambar-4. Alur proses enkripsi citra menggunakan transposisi kolom.

2) Enkripsi vigenere pada Citra

Setelah citra dilakukan enkripsi dengan transposisi kolom, citra kembali dienkripsi dengan algoritma *vigenere*. Pada tahap ini dibutuhkan sebuah kunci acak yang harus dibuat dengan fungsi random. Dimana nilai masing-masing kunci random dalam rentang 0 sampai 255 sesuai dengan nilai pixel citra. Berikut adalah langkah-langkah enkripsi yang diusulkan dengan algoritma *vigenere*.

1. Baca citra yang telah terenkripsi dengan transposisi kolom.
2. Buat kunci random dengan fungsi random pada matlab untuk menghasilkan barisan angka dalam rentang 0 sampai 255

menggunkan fungsi modulo. Dengan ukuran barisan menyesuaikan citra terenkripsi transposisi kolom. Lalu simpan kunci tersebut untuk dikirim ke penerima pesan.

3. Lakukan proses enkripsi pada citra terenkripsi transposisi kolom dengan kunci random menggunakan persamaan (1).

C. Dekripsi Citra

Karena tahap enkripsi citra dilakukan menggunakan dua metode maka pada proses dekripsi juga akan dilakukan menggunakan dua metode. Proses dekripsi dilakukan pada sisi penerima pesan.

1) Dekripsi vigenere chipper

Pada langkah dekripsi citra berkebalikan dengan enkripsi citra. Karena proses enkripsi diawali dengan algoritma transposisi kolom dilanjutjan dengan *Vigenere chipper*. Maka pada proses dekripsi berkebalikan. *Vigenere chipper* dilakukan terlebih dahulu untuk membaca citra yang telah terenkripsi. Berikut adalah langkah-langkah dekripsi yang diusulkan dengan algoritma *vigenere*.

1. Baca citra yang telah terenkripsi.
2. Baca kunci random yang telah dikirimkan pengirim.
3. Lakukan proses dekripsi pada citra terenkripsi dengan kunci random menggunakan persamaan (2).

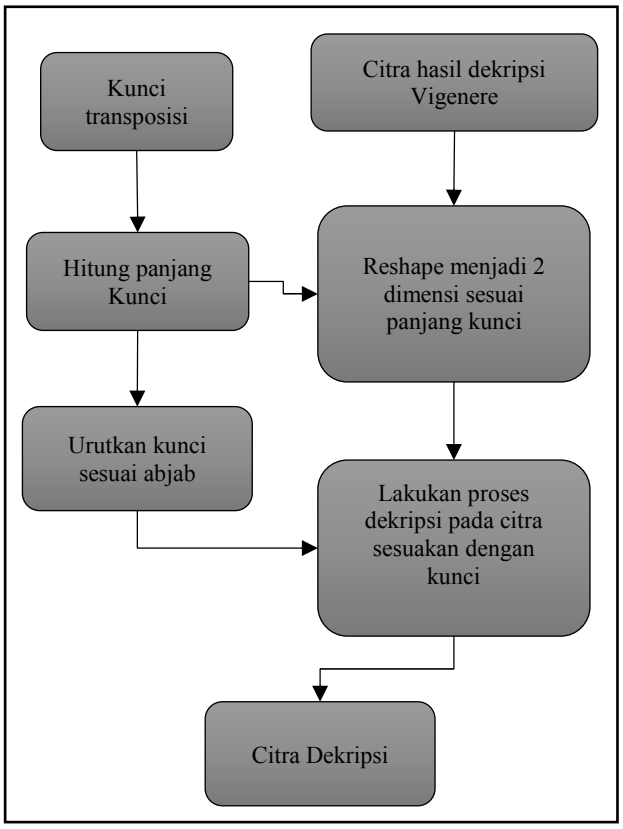
2) Dekripsi transposisi kolom pada Citra

Proses dekripsi transposisi kolom pada citra tentunya juga berbeda dengan file teks. Perbedaan ini dikarenakan dimensi citra dan teks berbeda. Pesan teks berdimensi satu, sedangn citra berdimensi dua untuk citra keabuan sedangkan citra berwarna berdisensi tiga.

Berikut adalah langkah detil dari proses enkripsi citra dengan transposisi kolom.

1. Baca citra hasil dekripsi *vigenere*.
2. Inputkan kunci berupa teks, sesuaikan dengan proses enkripsi.
3. Ubah citra menjadi dua dimensi sesuai dengan panjang kunci untuk jumlah kolom dan jumlah baris yang menyesuaikan.
4. Urutkan abjad kunci.
5. Lakukan dekripsi sesuai dengan urutan abjad kunci.
6. Dapatkan citra terdekripsi.

Untuk melihat lebih detil deskripsi langkah-langkah transposisi dapat dilihat pada Gambar-5.



Gambar-5. Alur proses dekrispi citra menggunakan transposisi kolom.

D. Pengujian dan evaluasi metode

Seletah metode berhasil dilakukan, maka dilakukan proses pengujian dan evaluasi. Tahap ini hasil enkripsi akan diukur dengan entropy, sedangkan untuk hasil dekripsi citra akan diukur dengan PSNR dan SSIM. PSNR dan SSIM diukur dengan membandingkan citra asli dengan citra setelah dienkripsi. Semakin tinggi nilai PSNR maka kualitas citra hasil dekripsi semakin mirip dengan citra asli. Apabila nilai PSNR tak terhingga maka citra hasil dekripsi dama persis dengan citra asli dan hal ini membuktikan bahwa proses dekripsi berjalan dengan baik. Persamaan (3) digunakan untuk menghitung PSNR [15].

$$PSNR_{dB}=10\log_{10}\left(\frac{255^2}{MSE}\right) \quad (3)$$

Dimana:

MSE didapatkan dengan persamaan (4)

$$MSE=\sum_{h=1}^{H-1}\sum_{g=1}^{G-1}\|A(h,g)-B(h,g)\| \quad (4)$$

Dimana:

H dan G adalah ukuran citra

A merupakan citra asli

B merupakan citra hasil dekripsi

SSIM juga mirip dengan PSNR, hanya saja rentang nilainya dari 0 hingga 1. Nilai 1 berarti citra asli sama dengan citra dekripsi. Persamaan (5) digunakan untuk menghitung SSIM.

$$SSIM\ (A,B)= \frac{(2\mu_A\mu_B+c_1)(2\sigma_{AB}+c_2)}{(\mu_A^2+\mu_B^2+c_1)(\sigma_A^2+\sigma_B^2+c_2)} \qquad (5)$$

Dimana:
A adalah citra asli
B adalah citra hasil dekripsi
μ_A dan μ_B adalah nilai mean A dan B
σ_{AB} adalah covriant A dari B
σ_A^2 adalah variant dari A
σ_B^2 adalah variant dari B
$c_1=(k_1L)^2$ dan $c_2=(k_2L)^2$.

L adalah nilai dinamik dari citra $(2^{bit}-1)$ dengan nilai default $k_1=0{,}01$ dan $k_2=0{,}03$.

Performa kecepatan kalkulasi metode juga diukur dengan dengan fungsi tic toc pada MATLAB.

IV. HASIL DAN PEMBAHASAN

A. Hasil Pra Pengolahan Bab

Sesuai dengan metode yang telah disulakan diatas maka sebelum dilakukan pengujian. Citra di *resize* menggunakan fungsi *imresize* yang ada di matlab. dengan empat ukuran yang berbeda. Hal ini dilakukan untuk menguji performa metode pada ukuran citra yang berbeda. Gambar-6 menunjukan sampel hasil proses *resize* pada citra *cameraman*.

(a) (b) (c) (d)

Gambar-6. Hasil proses pra pengolahan.

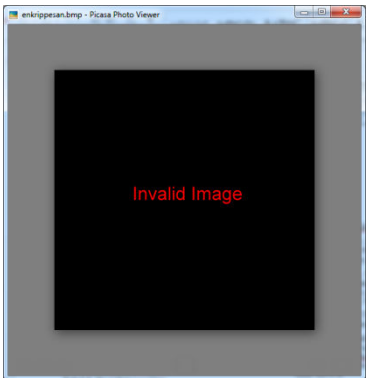
B. Hasil Pengujian Enkripsi Citra

Setelah dilakukan pra pengolahan, maka masing-masing citra dengan berbagai ukuran akan diujicobakan dengan metode yang telah diusulkan. Tabel-1 menunjukkan waktu yang dibutuhkan untuk melakukan enkripsi.

Tabel-1. Hasil Enkripsi Citra.

Nama Citra	Ukuran (piksel)	Waktu Proses (detik)
Barbara	1024*1024	9,962254
	512*512	1,578365
	256*256	0,377351
	128*128	0,108719
Cameraman	1024*1024	10,036611
	512*512	1,559925
	256*256	0,368647
	128*128	0,126857
F16	1024*1024	9,825684
	512*512	1,572116
	256*256	0,350288
	128*128	0,116242
Goldhill	1024*1024	10,095485
	512*512	1,575840
	256*256	0,373461
	128*128	0,113800
Lena	1024*1024	9,879591
	512*512	1,565077
	256*256	0,368741
	128*128	0,100510
Pentagon	1024*1024	10,148356
	512*512	1,566223
	256*256	0,362755
	128*128	0,111723

Setelah citra dienkripsi bentuk citra berubah tidak seperti aslinya tapi tetap memiliki format yang sama. Tetapi citra ini tidak dapat ditampilkan pada beberapa aplikasi seperti picasa. Gambar-7 menunjukan citra hasil enkripsi ketika dibuka dengan aplikasi Picasa.



Gambar-7. Tampilan citra hasil enkripsi ketika dibuka dengan aplikasi Picasa.

C. Hasil Pengujian Dekripsi Citra

Setelah dilakukan proses enkripsi, maka masing-masing citra dengan berbagai ukuran akan didekripsi dengan metode yang telah diusulkan. Tabel-2 waktu yang dibutuhkan untuk melakukan enkripsi, SSIM, dan PSNR.

Tabel-2. Hasil dekripsi citra.

Nama Citra	Ukuran (piksel)	PSNR (Db)	SSIM	Waktu Proses (detik)
Barbara	1024*1024	inf	1	13,008994
	512*512	inf	1	0,916053
	256*256	inf	1	0,083905
	128*128	inf	1	0,015845
Cameraman	1024*1024	inf	1	12,791357
	512*512	inf	1	0,898819
	256*256	inf	1	0,118653
	128*128	inf	1	0,015147
F16	1024*1024	inf	1	13,058064
	512*512	inf	1	0,896962
	256*256	inf	1	0,083602
	128*128	inf	1	0,015326
Goldhill	1024*1024	inf	1	13,331752
	512*512	inf	1	0,898415
	256*256	inf	1	0,084729
	128*128	inf	1	0,015798
Lena	1024*1024	inf	1	13,067434
	512*512	inf	1	0,889487
	256*256	inf	1	0,085181
	128*128	inf	1	0,014647
Pentagon	1024*1024	inf	1	13,414928
	512*512	inf	1	0,886613
	256*256	inf	1	0,084490
	128*128	inf	1	0,018957

Penelitian lain yang telah dilakukan oleh Permana[16] menggunakan algoritma Vernam Cipher pada citra *grayscale* akan dijadikan paper pembanding dengan penelitian ini. Kesamaan citra yang digunakan pada ukuran 256x256 piksel dan kesamaan alat hitung yaitu PSNR maka dapat digambarkan hasil komparasi tersebut sesuai Tabel-3.

Tabel-3. Komparasi waktu dekripsi dengan penelitian lain pada ukuran piksel 256x256 piksel.

Nama Citra	Waktu Proses (detik)	
	Penelitian Terdahulu[16]	Metode Yang Kami Gunakan
F16	0,004029	0,083602

Dari hasil komparasi diketahui bahwa waktu ekseskusi proses dekripsi pesan lebih lama *vigenere cipher* dibandingkan dengan *vernam cipher* pada citra *grayscale* ukuran 256x256 piksel.

V. PENUTUP

A. Kesimpulan

Berdasarkan hasil eksperimen dan pembahasan yang telah dilakukan sebelumnya dapat disimpulkan bahwa metode yang telah diusulkan dapat bekerja dengan baik pada berbagai ukuran citra. Waktu yang dibutuhkan untuk proses enkripsi relatif sedikit lebih lama dibandingkan dengan proses dekripsi. Hasil proses enkripsi juga dapat membuat citra terkesan rusak sehingga tidak dapat dilihat menggunakan beberapa aplikasi seperti Picasa. Sedangkan proses dekripsi citra dapat bekerja dengan sempurna dimana dibuktikan dengan nilai PSNR yang tak terbatas (inf), ataupun dengan metode ukur SSIM dimana didapatkan nilai 1.

B. Saran

Berdasarkan hasil eksperimen, pada citra berukuran lebih dari 512*512 memerlukan waktu enkripsi yang cukup lama. Maka perlu dilakukan efektifitas algoritma agar komputasi dapat dilakukan dengan lebih cepat lagi.

DAFTAR PUSTAKA

[1] Setiadi DRIM, Rachmawanto EH, Sari CA,. Secure Image Steganography Algorithm Based on DCT with OTP Encryption. *Journal of Applied Intelligent System.* 2017; 2(1): 1-11.

[2] Winaryo FC, Wowor AD, Widiasari IR. *Implementasi Modifikasi Kriptografi One Time Pad (OTP) untuk Pengamanan Data File*. Salatiga: Repository UKSW. 2014.

[3] Najih M, Setiadi DRIM, Rachmawanto EH, Sari CA, Astuti S. *An Improved Secure Image Hiding Technique Using PN-Sequence Based On DCT-OTP*. International Conference on Informatics and Computational Sciences (ICICoS). Semarang. 2017.

[4] Fahrianto F, Masruroh SU, Ando NZ. *Encrypted SMS Application on Android with Combination of Caesar Cipher and Vigenere Algorithm.* International Conference on Cyber and IT Service Management (CITSM). Tangerang. 2014.

[5] Hannan SA, Asif AMAM. Analysis of Polyalphabetic Transposition Cipher Techniques used for Encryption and Decryption. *International Journal of Computer Science and Software Engineering (IJCSSE).* 2017; 6(2) : 41-46.

[6] S. Garg, S. Khera, Aggarwa A. "Extended Vigenere Cipher with Stream Cipher," *International Journal of Engineering Science and Computing.* 2016; 6(5) : 5176-5180.

[7] Saputra I, Aan M, Hasibuan NA, Rahim R. Vigenere Cipher Algorithm with Grayscale Image Key Generator for Secure Text File. *International Journal of Engineering Research & Technology (IJERT).* 2017; 6(1) : 266-269.

[8] Kester QA. A cryptosystem based on Vigenère cipher with varying key. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET).* 2012; 1(10) : 108-113.

[9] Soofi AA, Riaz I, Rasheed U. An Enhanced Vigenere Cipher For Data Security. *International Journal of Scientific and Technology Research.* 2016; 5(3) : 141-145.

[10] Katz J, Lindell Y. Introduction to Modern Cryptography. CRC Press. 2014 .

[11] Munir R, Riyanto B, Sutikno S. *Perancangan Algoritma Kriptografi Stream Cipher dengan Chaos*. Prosiding Seminar Nasional: KNSI. Bandung.2006.

[12] Nani PA. *Penerapan Enkripsi Algoritma Blowfish Pada Proses Steganografi Metode EOF*. Prosiding SNATIKA. 2011.

[13] Heydari M, Shabgahi GL, Heydari MM. Cryptanalysis of Transposition Ciphers with Long Key Lengths Using an Improved Genetic Algorithm. *World Applied Sciences Journal.* 2013; 21(8) : 1194-1199.

[14] Pramanik MB. Implementation of Cryptography Technique using Columnar Transposition. *International Journal of Computer Applications (0975 – 8887).* 2014 : 19-23.

[15] Irawan C, Setiadi DRIM, Sari CA, Rachmawanto EH. *Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption*. International Conference on Informatics and Computational Sciences (ICICoS). Semarang. 2017.